OIPE
JUL 31 2006
IAP69
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Inventors: Gadiel Seroussi et al.

Serial No. 09/916,785

Filed: July 27, 2001

For: METHOD AND APPARATUS FOR RANDOM BIT-STRING GENERATION USING ENVIRONMENT SENSORS

Examiner: Jeffery L. Williams

Group Art Unit: 2137

Docket No. 10010554-1

Date: July 27, 2006

AMENDED APPEAL BRIEF

Mail Stop: Appeal Briefs – Patents
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Examiner, in an Office Action mailed October 3, 2005, finally rejecting claims 10-13.

REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

Applicants' representative has not identified, and does not know of, any other appeals of interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 10-13 are pending in the application. Claims 1-9 have been canceled. Claims 10-13 were finally rejected in the Office Action dated October 3, 2005. Applicants appeal the final rejection of claims 10-13, which are copied in the attached CLAIMS APPENDIX.

STATUS OF AMENDMENTS

An Amendment After Final is enclosed with this brief amending claims 10 and 11. In the Office Action dated October 3, 2005, the Examiner rejected claims 10-13 under 35 U.S.C. §112, ¶2 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Accordingly, Applicants' representative amended claims 10 and 11 to overcome the Examiner's rejections of claims 10 and 11. In an Advisory Action of June 27, 2006, the Examiner indicated that the amended claim 11 lacked antecedent basis for the language "the additional compressors" and indicated that the amended claim 11 now recited multiple additional compressors for each additional sensor. Applicants did not intend that amended claim 11 be read as the Examiner appears to have read amended claim 11, and do not feel that amended claim 11 recites multiple additional compressors for any particular environmental sensor, but Applicants also appreciate the Examiner's concern and diligent reading of the claim, and acknowledge that the originally amended claim 11 could be viewed as ambiguous. Applicants therefore submit an amended Appeal Brief and a newly amended claim 11 in which the word "compressors" has been replaced by the word "compressor," in order to remove any ambiguity as to the meaning of amended claim 11. The current amendments to claims 10 and 11 are reflected in the CLAIMS APPENDIX.

SUMMARY OF CLAIMED SUBJECT MATTER

Overview

Claims 10-14 are directed to a random number generator shown in Figure 1 of the current application. As shown in Figure 1, digitally encoded input from one or more environmental sensors (11 in Figure 1) are input into one or more corresponding compressors (12 in Figure 1) that compress the received digitally encoded data from the sensors to generate compressed data streams. The compressed data streams are merged by a merge circuit (13 in Figure 1). The merge circuit merges the compressed data streams received from the compressors, and also monitors the resulting merged bit stream to ensure that sufficient bits are produced in the compressed streams to satisfy uncertainty requirements before allowing a next random number to be generated and produced by the random number generator. A hash generator (15 in Figure 1) receives bits from the merged compressed data stream and generates an output block of bits that are output as next random number. The merge circuit (13 in Figure 1) controls a blocking switch (17 in Figure 1) to block output of a next random number until the merge circuit has received sufficient number of bits from the compressors that meet certain statistical requirements.

Independent Claim 10

Claim 10 is directed to a random number generation device such as that shown in Figure 1, described above. Claim 10 claims an environmental sensor (11 in Figure 1), a compressor (12 in Figure 1), a monitor (13 in Figure 1), a random number generator (15 in Figure 1), and a blocking switch (17 in Figure 1).

Dependent Claims 11-14

Dependent claim 11 adds additional sensors (11 in Figure 1) and compressors (12 in Figure 1). Independent claim 12 specifies that the random number generator (15 in Figure 1) applies a hash function to received data to produce a next random number. Independent claim 13 further specifies that the environmental sensors (11 in Figure 1) may be selected from a number of different, specific types of environmental sensors, including temperature, sound, motion, light-intensity, and ambient-electromagnetic-radiation sensors.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claim 12 is indefinite under 35 U.S.C. §112, ¶2.

2. Whether claims 10-13 are unpatentable over Eastlake et al., "Randomness Recommendations for Security," R.F.C. 1750 ("Eastlake") in view of Saints et al., U.S. Patent No. 6,430,170 ("Saints").

ARGUMENT

Claims 10-13 are pending in the current application. In an Office Action dated October 12, 2005 ("Office Action"), the Examiner rejected claims 10-13 under 35 U.S.C. §112, ¶2 as being indefinite, and rejected claims 10-13 as being unpatentable over Eastlake et al., "Randomness Recommendations for Security," R.F.C. 1750 ("Eastlake") in view of Saints et al., U.S. Patent No. 6,430,170 ("Saints") under 35 U.S.C. §103(a). Applicants respectfully traverse the 35 U.S.C. §112, ¶2 rejection of claim 12 and the 35 U.S.C. §103(a) rejections of claims 10-13.

ISSUE 1

1. Whether claim 12 is indefinite under 35 U.S.C. §112, ¶2.

Claim 10 recites "a random number generator that receives data from the compressed data stream." Claim 12 refers to the random number generator, introduced in claim 10, by reciting "the random number generator applies a hash function to the received data to produce a random number." In Applicants' representative's respectfully offered opinion, there is nothing indefinite in claim 12. The language "the received data" specifically refers to the data received by the random number generator, as recited in claim 10. The random number generator is not claimed to receive any other data in claims 10-12.

In rejecting claim 12, the Examiner states that "[a] random number generator that 'receives data,' as claimed in claim 10, does not adequately provide antecedent basis for 'the received data' as claimed." The Examiner does not provide any support for this statement in regulations or case law. Applicants' representative respectfully suggests that omitting the article "the" from claim 12, as suggested by the Examiner, would result in a significant

indefiniteness and ambiguity that is not present in claim 12 as originally submitted. In general, when referring to an element or entity previously introduced in an independent claim from a dependent claim, it is both necessary and customary to preface the recitation of the element or entity in the dependent claim by the definite article "the." By not so doing, as proposed by the Examiner, the phrase "received data" could refer to any received data except to the data received from the compressed data stream, as recited in claim 10.

ISSUE 2

2. Whether claims 10-13 are unpatentable over Eastlake et al., "Randomness Recommendations for Security," R.F.C. 1750 ("Eastlake") in view of Saints et al., U.S. Patent No. 6,430,170 ("Saints").

The Examiner relies primarily on Eastlake in rejecting claims 10-13 under 35 U.S.C. §103(a). In Applicants' representative's respectfully offered opinion, the Examiner reads far more into Eastlake than Eastlake explicitly states or represents. As one example, the Examiner states, in rejecting claim 10, that Eastlake discloses "a compressor that receives the digitally encoded sensor values generated by the environmental compressor and compresses the received digitally encoded sensor values to generate a compressed data stream" in Section 5.2. Eastlake does not teach such a compressor. Instead, Eastlake is a general, review article that mentions a variety of different security related techniques. Eastlake does mention using thermal noise as a physical source of unpredictable numbers, in Section 5, but does not teach, mention, or suggest using the physical source as a continuous source of random bits for generating a compressed data stream. Instead, in Section 5.1, Eastlake clearly indicates that Eastlake envisions using the physical source to obtain a sufficient number of random bits to occasionally generate strong random seeds, indicating that only a few hundred random bits per day would need to be obtained from the physical source to presumably generate a single strong random seed per day. Moreover, Section 5.1 refers to Section 6.3, in which Eastlake describes starting with a strong random seed, generated from a small number of random bits, and using the random seed as the initial input to a cryptographic system, or random-number generator, that generates a series of random quantities sequentially by a cryptographic random-number generator. Eastlake does not disclose a compressor that receives digitally encoded sensor values and generates from the digitally encoded sensor values a compressed data stream. In Section 5.2.4, Eastlake mentions using a reversible compression technique to

deskew a skewed bit stream. However, Eastlake does not, in Section 5.2.4, disclose or suggest the source of the bit stream, and does not suggest a compressed-data-stream output. Moreover, in Section 5.2.1, Eastlake computes a number of bits that need to be sampled in order to produce a deskewed result, indicating again that Eastlake envisions obtaining sufficient bits from a physical source to generate a seed, rather than a compressed stream of data. Finally, Eastlake makes no mention of a random number generator implementation that includes a compressor component that receives digitally encoded sensor values and that generates a compressed data stream.

In rejecting claim 10, the Examiner states that Eastlake discloses "a random number generator that receives data from the compressed data stream and outputs random numbers." Eastlake does indeed disclose, in Section 6, obtaining random input from a large number of uncorrelated sources and mixing them with a strong mixing function. However, Eastlake does not disclose that the large number of uncorrelated sources are compressed data streams. Instead, as explicitly disclosed by Eastlake in Section 6.3, Eastlake envisions using random bits, mixed by strong mixing functions, to generate a strong random seed that is the initial input into a cryptographic algorithm that then produces a series of random numbers. Thus, Applicants' representative respectfully disagrees that Eastlake discloses "a compressor that receives the digitally encoded sensor values generated by the environmental sensor and compresses the received digitally encoded sensor values to generate a compressed data stream."

In rejecting claim 10, the Examiner states that Eastlake does not disclose the monitor and blocking-switch elements of claim 10. The monitor claimed in claim 10 of the current application "receives the compressed data stream and monitors the compressed data stream to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number." The blocking switch claimed in claim 10 is "controlled by the monitor to block output of a next random number by the random number generator when sufficient data to generate the next random number has not been received in the compressed data stream to generate a next random number." The Examiner therefore turns to Saints, claiming that Saints discloses both the monitor and blocking-switch elements of claim 10.

Saints discloses a system and method for generating random numbers in a wireless communications network. Saints captures energy samples from signal noise, and processes the energy samples in order to generate random numbers. As discussed in Saints, beginning on line 51 of column 8, a pool of random numbers is initialized at power-up by mixing

energy samples with the contents of the pool, generally initialized to have all zero values. Moreover, as stated by Saints, beginning on line 57 of column 8, in a preferred embodiment, the pool buffer is large enough to store three random numbers. The pool, as discussed beginning on line 15 of column 9, contains bits provided by hashing energy samples with the current contents of the pool using a hashing algorithm (404 in Figure 4). Thus, the pool is not a compressed data steam generated from digitally encoded sensor values. Instead, the pool contains random numbers, generated by a hash function, from energy samples. The Examiner apparently relies on a single sentence from Saints, on lines 57-58 of column 9, for disclosing the monitor element of claim 10. That line states:

> In a preferred embodiment, as soon as the pool is filled, a random number will be extracted from the pool.

As explicitly stated by Saints, the pool generally contains multiple random numbers, and not a compressed data stream. This single sentence of Saints basically states that a buffer, or pool, of random numbers is first filled, and after the pool is filled, extraction of random numbers from the pool begins. There is no suggestion that a compressed data stream is continuously monitored by a monitor component to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number. Furthermore, in the first paragraph of column 10, Saints continues the description of the system by stating:

> It should be noted that once initialization of the pool is complete, and a number is extracted, a request for a number may be quickly filled. Once a number is extracted, the process to form a new number can begin. This enables the formation of the number to proceed at a lower priority than other processes in the subscriber unit, yet still assures good response when a number is required.

In other words, Saints discloses that, following pool initialization, subsequent random numbers are generally continuously available. Furthermore, since, in a preferred embodiment, the pool contains three already generated random numbers, it is clear that random number generation is not blocked until sufficient random bits to generate a next random number have been accumulated. When random number generation begins, in Saints system, three random numbers have already been generated and are available for extraction.

The cited passage of Saints, in combination with the preceding and following textual context from which it was taken by the Examiner, does not suggest a continuous monitoring of an input stream to determine whether or not sufficient data has been obtained to generate a

next random number. The cited passage merely described initialization of a random number buffer, or pool. Quite often, in automated systems, a first portion of a program execute, to initialize data structures and variables, before a steady-state, continuously executing portion of the program begins to execute. Such initialization code is not referred to as, nor considered as, a monitor. Initialization code generally executes once as the program begins execution, to prime execution of the bulk of the program, and is generally not subsequently executed during the remaining execution of the program. The cited passage of Saints describes such an initialization routine, and therefore does not describe, and is not relevant to, the claimed monitor that that receives the compressed data stream and monitors the compressed data stream to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number.

The Examiner apparently points to lines 30-59 of column 9 to teach both a monitor and a blocking switch. The monitor and blocking switch are discrete and separate components of the random number generator claimed in claim 10. There is no mention in lines 30-59 of column 9 of Saints of a blocking switch, or any other kind of switch. There is no mention in the cited lines of Saints that a monitor enables and disables random-number generation, using a blocking switch, as a result of monitoring an input compressed data stream. Instead, in the cited lines, as discussed above, Saints describes initialization of a buffer, or pool, which contains already generated random numbers and explicitly states that once the pool is initialized, successive random numbers can be quickly obtained. In short, Saints teaches neither a monitor nor a blocking switch in the cited lines of column 9. The fact that the steady state portion of Saints system does not begin execution until after pool initialization does disclose or suggest a blocking switch, any more than a program that first declares a loop variable and initializes the loop variable to "0" or "1," and then executes the loop, contains a blocking switch controlled by a monitor to control operation of the loop.

In justifying the combination of Eastlake and Saints, the Examiner states that:

> It would have been obvious to one of ordinary skill in the art to combine the method of Saints et al. (for providing a monitor to monitor the collection of random data in a blocking switch to prevent random number generation until sufficient random data has been collected) with the recommended methods of Eastlake et al. This would have been obvious because one of ordinary skill in the art would have been motivated to generate a "quality" random number by preventing ("blocking") a system from generating a random number if an insufficient amount of time has passed for the gathering of random input data in order to generate such a "quality" number.

As discussed above, Saints neither discloses, teaches, mentions, nor suggests a monitor to monitor the collection of random data and neither discloses, teaches, mentions, nor suggests a blocking switch to prevent random number generation until sufficient random data has been collected. Instead, the single sentence from column 9 to which the Examiner appears to attribute these components of the claimed random number generator simply states that a random number can be extracted from a pool of generated random numbers once the pool of generated random numbers is filled. The Examiner repeatedly refers to the term "quality random number," although Applicants' representative cannot find this term in either of the cited references or the current application. The justification for combination is thus, in part, based on a term that is not defined by the Examiner, and that does not appear to occur in either the cited references of the current application.

The Examiner finds that one skilled in the art would have been motivated to block generation of random numbers if an insufficient amount of time has passed for gathering of random input data in order to generate a quality number. Applicants' representative cannot find a teaching in Eastlake or Saints for blocking random number generation for a time sufficient to generate a quality number, and Applicants' clearly disclosed and claimed random number generator blocks generation of a next random until a sufficient number of random bits have been received, and not for specific periods of time. When the bits are available, no blocking occurs. Neither Eastlake nor Saints teaches, mentions, or suggests any kind of blocking of random number generation based on waiting a sufficient amount of time for gathering sufficient random input data. Eastlake does analyze a number of random bits needed for generating a strong cryptographic seed value, but does not teach, mention, or suggest a blocking component within a system that would block random number generation until a sufficient number of random bits have been received. Furthermore, the only portion of Saints cited by the Examiner concerns generating a sufficient number of random numbers to fill a pool of random numbers, in a pool-initialization process, before beginning to produce random numbers as output. The cited portion of Saints does not disclose or suggest a monitor and blocking switch that together wait a sufficient amount of time to generate a random number from the compressed output of an environmental sensor.

Regarding the rejection of claim 11, the Examiner states that Eastlake discloses "one or more additional environmental sensors" because Eastlake discloses a method of mixing together the random input gathered by such sensors. Applicants' representative believes that

the Examiner is referring to the following paragraph from Section 6 of Eastlake:

> What is the best overall strategy for meeting the requirement for unguessable random numbers in the absence of a reliable hardware source? It is to obtain random input from a large number of uncorrelated sources and to mix them with a strong mixing function.

This statement has nothing at all to do with environmental sensors or mixing together the random input of environmental sensors. Instead, as the title for the section, "Recommended Non-Hardware Strategy," suggests, this section of Eastlake refers to using strong mixing functions to mix pseudorandom numbers from various sources together to produce a more random output. Eastlake is referring to non-hardware pseudorandom number sources, rather than to sensors or other such physical devices. The Examiner then states that Eastlake discloses "an additional compressor for each of the one or more additional environmental sensors." As discussed above, Eastlake does not even disclose a single compressor component for a random-number-generator device.

Regarding the rejection of claim 13, the Examiner cites several sections of Eastlake that refer to several sources of random bits. Section 4.2 suggests arrival of keystrokes or network packets. Section 5 mentions a thermal noise source. Section 5.3.1, alternative thermal noise sources are discussed, including a camera covered by a lens cap and a sound digitizer with no source plugged in. From these modest suggests that include essentially only one type of environmental sensor, namely a thermal noise sensor, the Examiner finds the more extensive list of physical sources for random bits in claim 13 to be obvious. Applicants' representative respectfully observes that obviousness-type rejects require at least a clear suggestion, and that a thermal sensor does not suggest sound, motion, light-intensity, and electromagnetic radiation sensors.

In general, claims 11-13 depend from claim 10, and since claim 10 is not made obvious be either Eastlake, Saints, or Eastlake and Saints in combination, claims 11-13 are also not obvious

CONCLUSION

Claim 12, as submitted, is not indefinite, and the Examiner's proposed amendment to claim 12 would result in the amended claim being substantially indefinite. Eastlake is a review article discussing various methods and characteristics of various methods employed for random number generation. Eastlake neither discloses nor suggests Applicants'

claimed random number generator. Saints discloses a random number generator, but discloses neither the claimed monitor nor claim blocking switch recited in claim 10, and included in claims 11-13 by dependency from claim 10. Claims 10-13 are not obvious in view of either of the cited references alone, or in combination.

Applicant respectfully submits that all statutory requirements are met and that the present application is allowable over all the references of record. Therefore, Applicant respectfully requests that the present application be passed to issue.

Respectfully submitted,
Gadiel Seroussi et al.
OLYMPIC PATENT WORKS PLLC

By ____________________
Robert W. Bergstrom
Registration No. 39,906

CLAIMS APPENDIX

Claims 1-9 canceled.

10. A random number generation device comprising:

an environmental sensor that generates digitally encoded sensor values;

a compressor that receives the digitally encoded sensor values generated by the environmental sensor and compresses the received digitally encoded sensor values to generate a compressed data stream;

a monitor that receives the compressed data stream and monitors the compressed data stream to determine whether or not sufficient data has been received in the compressed data stream to generate a next random number;

a random number generator that receives data from the compressed data stream and outputs random numbers; and

a blocking switch controlled by the monitor to block output of a next random number by the random number generator when sufficient data to generate the next random number has not been received in the compressed data stream to generate a next random number.

11. The random number generation device of claim 10 further comprising:

one or more additional environmental sensors;

an additional compressor for each of the one or more additional environmental sensors; and

a merging component that merges compressed data streams output by the compressor and the additional compressor for each of the one or more additional environmental sensors to produce a merged, compressed data stream that is output to the monitor and random number generator.

12. The random number generation device of claim 11 wherein the random number generator applies a hash function to the received data to produce a random number for output by the random number generation device.

13. The random number generation device of claim 11 wherein each environmental sensor monitors an environmental parameter, the environmental parameter selected from among

environmental parameters including:

temperature;

sound;

motion;

light intensity; and

ambient electromagnetic radiation.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.